THE CENTRE FOR HUMANITARIAN DATA

GUIDANCE NOTE SERIES
DATA RESPONSIBILITY IN HUMANITARIAN ACTION

GUIDANCE NOTE ON THE IMPLICATIONS OF CYBER THREATS FOR HUMANITARIANS

KEY TAKEAWAYS:

- Cyber threats are one of the most pressing issues facing the humanitarian sector today. Digital transformation, increasing dependence on information and communications technology, and the prevalence of cyber threats create a new array of risks for humanitarian agencies and the people they serve.
- Cyber threats comprise a variety of activities and behaviors that can be distinguished by the types of actors behind them and their motives, as well as the type of threat.
- Common vulnerabilities in the humanitarian sector include infrastructure flaws, inadequate basic cybersecurity and digital literacy, human error and the absence of coordinated approaches.
- Cyber threats can compromise humanitarians' ability to deliver assistance and protect affected populations. They directly affect a number of key humanitarian programming areas, including protection, access, and accountability to affected populations and communicating with communities.
- In order to improve cyber resilience, organizations should invest in cybersecurity as a cross-organizational issue, enhance institutional preparedness, increase digital literacy of staff, and improve coordination and collaboration.

INTRODUCTION

Humanitarian organizations rely more than ever on digital technologies to assist and protect people in crisis.[1] These technologies enable humanitarians to gather data to understand and respond to the needs of affected people, and offer new channels to deliver aid through unprecedented digital proximity.[2] However, this increased digitalization is not without risks—chief among them is the growing risk of cyber threats.[3]

Cyber threats are one of the most pressing issues facing the humanitarian sector today.[4] Digital transformation, increasing dependence on information and communications technology (ICT), and the prevalence of cyber threats create a new array of risks for humanitarian agencies and the people they serve. A few examples include:

[1] NetHope (2022). **Humanitarians (and data) #NotATarget**.

[2] Massimo Marelli and Adrian Perrig (2020). **Hacking Humanitarians: Mapping The Cyber Environment And Threat Landscape**, International Committee of the Red Cross, 7 May.

[3] UNOCHA GHPF (2022). **Virtual Risk, Tangible Harm: The Humanitarian Implications of Cyber Threats**.

[4] World Economic Forum (2022). **The Global Risks Report 2022 17th Edition**. Geneva.

- In April 2020, at the beginning of the COVID-19 pandemic, Mercy Corps and the International Federation of Red Cross and Red Crescent Societies (IFRC) reported a drastic uptick in data protection breaches,[5] and the World Health Organization (WHO) noted a fivefold increase in the number of cyber threats against the organization.[6]

- In May 2021, hackers gained access to the email marketing account of the United States Agency for International Development (USAID), emailing over 150 organizations in an apparent attempt to hack them.[7]

- In February 2022, a highly targeted cyber operation against servers of the International Committee of the Red Cross (ICRC) which compromised sensitive data of more than 515,000 individuals was detected.[8]

These attacks may cause serious harm. They violate the privacy of the people whose data is compromised, risk exposing sensitive information about them and erode trust in humanitarian organizations' capabilities.

In response to these attacks, a number of new initiatives signal increased investment in this area. For example, ICRC is considering the development of a 'digital emblem'[9] and has also opened a new delegation for cyberspace in Luxembourg.[10] NetHope has established an Information Sharing and Analysis Center that will help support the information security needs of nonprofit agencies and the world's most vulnerable communities.[11] However, the sector lacks a shared approach to mitigating the risk and potential impact of cyber threats.

This Guidance Note aims to help build a common understanding and support more strategic, collective action within the sector. It provides an overview of the cyber threats, vulnerabilities, and implications facing humanitarians and people affected by crises, and offers recommendations to increase cyber resilience within and across organizations and their partners.

Definitions

Cybersecurity entails a combination of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment, and organization and user assets against relevant security risks in the cyber environment.[12]

Information and data security entails a set of physical, technological and procedural measures that safeguard the confidentiality, integrity and availability of data, and prevent its accidental or intentional, unlawful or otherwise unauthorized loss, destruction, alteration, acquisition or disclosure.[13]

Cyber threats encompass 'activities that occur at least in part within the cyber realm, utilizing and/or targeting information communications technologies to achieve an effect that is not authorized by the legitimate user of the data or the ICT and/or has a harmful intent or effect on the victim or victims'.[14]

Cyber resilience refers to an organization's capacity to identify, prevent and detect cyber threats, and respond and recover.

[5] Rebecca Root (2020). **COVID-19 Brings Wave of Cyberattacks Against NGOs**, Devex, 13 April.

[6] World Health Organization (2020). **WHO Reports Fivefold Increase in Cyberattacks, Urges Vigilance**, 23 April.

[7] Kelly Sheridan (2021). **US Seizes Attacker Domains Used in USAID Phishing Campaig**n, DARKReading, 1 June; Adva Saldinger (2021). **USAID Hack is 'Wakeup Call' for Aid Industry on Cybersecurity**, Devex, 4 June.

[8] International Committee of the Red Cross (2022). **Cyber-Attack on ICRC: What We Know**, 16 February.

[9] ICRC (2022). **ICRC proposes digital red cross/crescent emblem to signal protection in cyberspace**, 3 November. Linked to this is the notion of the "sovereign cloud" - i.e., a cloud architecture in which data sovereignty can be respected and applied. See ICRC (2020). **Handbook on Data Protection in Humanitarian Action**.

[10] ICRC (2022). **The ICRC opens a new delegation for cyberspace in Luxembourg**, 17 November.

[11] NetHope (2022). **Digital Protection and Cybersecurity**.

[12] Adapted from: International Telecommunication Union (ITU) Recommendation ITU-T X.1205, **Overview of cybersecurity.**

[13] IASC, 2021. **Operational Guidance on Data Responsibility in Humanitarian Action**.

[14] UNOCHA GHPF (2022). **Virtual Risk, Tangible Harm: The Humanitarian Implications of Cyber Threats**.

CYBER THREATS

To increase cybersecurity within the sector, organizations must first understand the threats they may face in this sphere. Cyber threats comprise a wide variety of activities and behaviors that can be distinguished by the types of actors behind them and their motives. Actors range from nation-states to criminal organizations and private persons or combinations thereof. The affiliation and goals of actors can inform how aggressively they behave, how sophisticated attacks are, which methods are used and who is targeted.

Cyber threats can be direct or indirect, depending on the target. Direct cyber threats, which target humanitarian organizations, have increased in recent years. Indirect cyber threats target the infrastructure or services that people affected by or responding to humanitarian crises rely on for survival and aid delivery.

Cyber threats can also be classified according to their type or mode. These include Denial-of-service (DoS) and Distributed denial-of-service (DDoS) attacks,[15] malware,[16] and ransomware,[17] among others.

The following examples illustrate what cyber threats might look like in practice:

- **Cyber warfare** refers to 'operations against a computer, a computer system or network, or another connected device, through a data stream, when used as means or methods of warfare in the context of an armed conflict'.[18] In Ukraine, cyber-attacks have undermined the distribution of medicines, food and relief supplies since February 2022.[19] Their impact has ranged from preventing access to basic services to data theft and disinformation.

- **Misinformation, disinformation and hate speech (MDH)** refers to the organized dissemination (intentional or unintentional) of false information through means of ICT which discredits political, military or civil society actors, or spreads, incites, promotes or justifies hatred and violence based on intolerance. In Myanmar, a campaign of MDH with derogatory and dehumanizing language against the Rohingya Muslim minority of the country has been linked to the commission of grave human rights violations.[20]

- **Cybercrime** refers to criminal offenses that are cyber-enabled (committed through the means of ICT) or cyber-dependent (only possible because of ICT).

- **Cyber sabotage** refers to activities aiming to disrupt or destroy the reliable and error-free functioning of ICT. If an act of sabotage is carried out by perpetrators with terrorist motives, it is referred to as cyber terrorism.

[15] Denial-of-service (DoS) and Distributed denial-of-service (DDoS) attacks flood a system's resources, overwhelming them and preventing responses to service requests, which reduces the system's ability to perform. (**Source: IBM**).

[16] Malware is malicious software that can render infected systems inoperable. Most malware variants destroy data by deleting or wiping files critical to the operating system's ability to run. (**Source: IBM**).

[17] Ransomware is sophisticated malware that takes advantage of system weaknesses, using strong encryption to hold data or system functionality hostage. Cybercriminals use ransomware to demand payment in exchange for releasing the system. A recent development with ransomware is the add-on of extortion tactics. (**Source: IBM**).

[18] International Committee of the Red Cross (November 2019). **International Humanitarian Law and the Challenges of Contemporary Armed Conflicts: Recommitting to Protection in Armed Conflict on the 70th Anniversary of the Geneva Conventions**.

[19] European Parliamentary Research Service (June 2022). **Russia's war on Ukraine: Timeline of cyber-attacks**.

[20] UN. **Hate speech and real harm**; Human Rights Council (2018). **Report of the Independent International Fact-finding Mission on Myanmar** (A/HRC/39/64).

COMMON VULNERABILITIES IN THE HUMANITARIAN SECTOR

Humanitarian actors should investigate and understand potential vulnerabilities that might impact their cyber resilience, and make them more susceptible to becoming victims of cyber threats. These include infrastructure flaws, inadequate basic cybersecurity and digital literacy, human error and the absence of a coordinated approach.

1. Infrastructure flaws

Cyber threats are commonly associated with sophisticated technical operations targeting vulnerabilities in information infrastructure.[21] Common vulnerabilities of this type relevant to the humanitarian sector include:

- **Legacy systems:** Outdated computing software and/or hardware that are unable to resist contemporary forms of attack, and present a risk for other applications and data that may share the same infrastructure.[22]

- **Default or improper configuration:** Out-of-box systems, i.e., with default or simple passwords and overly permissive configurations are easier for attackers to compromise.[23]

- **Lack of encryption:** In the absence of encryption, attackers can use software to discover usernames and passwords. A lack of encryption means that an attacker can access the data on compromised devices. Data that is transferred via unencrypted channels is also at risk of unauthorized access.

- **Third-party infrastructure:** Attackers can infiltrate ICT systems through an outside partner or vendor by exploiting different vulnerabilities.[24] Attackers may also gain access to the data stored by providers. Disruption of critical infrastructure through cyber operations can lead to a shutdown of essential services, which can have grave consequences for people in need and disrupt humanitarian operations.[25] Vendor lock-in due to product incompatibilities, low levels of interoperability or portability, or limited alternatives in the market are also major concerns.[26]

2. Inadequate basic cybersecurity and digital literacy

Cybersecurity preparedness, organizational readiness and digital literacy remain limited in the humanitarian sector.[27] Inadequate data literacy, and a lack of consistent practices and tools to ensure cybersecurity are widespread among humanitarian organizations. Cybersecurity continues to be seen as a predominantly technical issue, leading to little engagement from staff or leadership to raise awareness of threats and equip people across organizations with the skills and tools required to mitigate risk. This lack of engagement and focus also translates into a lack of resources and funding for cybersecurity.[28] Even as humanitarian actors digitalize their operations, gaps remain between the investment in the front end of technology (building it, deploying it, and closing out the project), and the back end (maintaining services and keeping information secure and protected over time).[29]

[21] UN (2021). **Cybersecurity in the United Nations system organizations: Report of the Joint Inspection Unit**.

[22] UN (2021). **Cybersecurity in the United Nations system organizations: Report of the Joint Inspection Unit**.

[23] Checkpoint (2020). **Critical Infrastructure and SCADA/ICS Cybersecurity Vulnerabilities and Threats**.

[24] Massimo Marelli (2021). **The SolarWinds hack: lessons for humanitarians**. International Committee of the Red Cross, 18 May.

[25] Between June 2020 and April 2022, the **CyberPeace Institute analyzed** data on 379 cyber-attacks against the healthcare sector across 36 countries with an average of 165,000 records breached per incident—and this is a mere fraction of the full extent of the problem. In 2015, a **sophisticated malware operation targeting Ukraine's electricity grid** left 230,000 residents without power for up to six hours in the middle of winter, in the first confirmed hack to take down a power grid. Israel's national water provider Mekorot **reported** in 2021 that its water networks are subject to "several hundreds of thousands of hacking attempts" per year. In February 2022, satellite communications firm Viasat **reported** a suspected cyber-attack that resulted in a partial outage of residential broadband services in Ukraine and other European countries. Noëlle van der Waag-Cowling (2022). **Living Below the Cyber Poverty Line: Strategic Challenges for Africa**, ICRC Humanitarian Law & Policy Blog, 11 June.

[26] Massimo Marelli (2021). **The SolarWinds hack: lessons for humanitarians**. International Committee of the Red Cross, 18 May.

[27] UN GHPF (2021). **The Humanitarian Implications of Cyber Threats**.

[28] WEF (2022). **Why the humanitarian sector needs to make cybersecurity a priority**, 17 January.

[29] Catherine Cheney (2022). **Delivering digital aid when the internet becomes a weapon of war**, DevEx, 28 January.

3. Human error

There has been a discernible shift from hackers attacking servers, networks and devices to 'hacking people' in recent years.[30] Ninety-five percent of cybersecurity breaches are now caused by human error.[31] Social engineering techniques (phishing, impersonation, etc.) aimed at manipulating individuals into divulging sensitive information are the most prevalent means of exploiting this vulnerability. Most of these techniques are designed to reach a high number of users simultaneously, maximizing the likelihood of a breach. These intrusions can go undetected for extended periods of time, giving attackers access to internal security architecture and confidential information, which in turn offers further opportunities for attack.

Human error that increases vulnerability to cyber threats may include:

- accidental abuse by users with authorized and legitimate access to computer systems;
- unauthorized use by attackers enabled by a compromised user;
- disregard by personnel for security policies and procedures; and
- errors in the configuration or operation of systems.

4. Absence of coordinated approach

There is an acute gap in coordination on cyber-related issues in the humanitarian sector. This gap exists both within and between organizations. Few organizations have teams dedicated to cybersecurity or tasked with detecting, assessing and mitigating cyber risks. No single entity is formally tasked with coordinating a harmonized approach to cybersecurity in the sector, despite the existence of initiatives such as the ones described above, the development of resources and apparent political will.[32]

The lack of coordination means that organizations lack visibility on attacks experienced by their peers, are unable or do not have policies in place to consistently share information on experienced cyber threats or lessons learned, and are not investing in collective approaches to reducing vulnerabilities and mitigating risk.[33]

HUMANITARIAN IMPLICATIONS OF CYBER THREATS

The humanitarian implications of cyber threats are significant. They can compromise the ability to deliver assistance and protection, as well as exacerbate humanitarian needs by disrupting services essential for survival. Cyber threats can result in surveillance, discrimination, persecution and other harmful consequences for affected populations, exacerbate the insecurities of already vulnerable groups and individuals, erode trust and compromise the principled delivery of humanitarian assistance.[34]

Delivering principled aid means that humanitarian services and assistance are aligned with the principles of humanity, neutrality, impartiality and independence.[35] To act with neutrality in the digital realm, humanitarian actors 'must ensure that the data and systems they employ do not provide any tactical military or operational advantage to parties engaged in hostilities'.[36] The humanitarian principle of independence might be in conflict with the dependence of ICT-supported humanitarian work on infrastructure owned and managed by private companies affiliated with different states. The overarching principle of 'Do No Harm' further obliges all humanitarians to avoid exposing people to additional risks

[30] UN (2021). Cybersecurity in the United Nations system organizations: Report of the Joint Inspection Unit.

[31] WEF (2020). After reading, writing and arithmetic, the 4th 'r' of literacy is cyber-risk.

[32] UN (2021). Cybersecurity in the United Nations system organizations: Report of the Joint Inspection Unit.

[33] One notable example of communication about cyber breaches was the ICRC's reaction to the 2022 cyber-attack, about which the organization communicated in a very transparent and timely manner, keeping partners and beneficiaries informed to the best of their abilities.

[34] UNOCHA GHPF (2022). Virtual Risk, Tangible Harm: The Humanitarian Implications of Cyber Threats.

[35] UNOCHA on Message: Humanitarian Principles.

[36] Brittany Card. (2015). Applying Humanitarian Principles To Current Uses Of Information Communication Technologies: Gaps In Doctrine And Challenges To Practice.Signal Program on Human Security and Technology, Harvard Humanitarian Initiative.

through humanitarian action, requiring humanitarians to take a step back from an intervention to look at the broader context and mitigate potential negative effects.[37]

Cyber threats directly affect a number of key humanitarian domains, such as protection, access, and accountability to affected people (AAP) and communicating with communities (CwC). As the technical tools for managing data in these different areas have evolved faster than the policy instruments that govern their use, organizations must exercise caution as they design and deploy digital technologies. The sections below offer considerations to help organizations better understand and address the humanitarian implications of cyber threats across these domains.

1. Protection

For humanitarian organizations, protection entails advocating for and supporting actions that aim to reduce and prevent people's exposure to risks and to ensure respect for the rights of individuals by those responsible.[38] Humanitarians must consider how cyber threats and related vulnerabilities impact their protection responsibilities, what effects technology might have on the distribution of resources, and how reliance on cyber infrastructure and vendors is redefining relationships.[39]

Information about the location of vulnerable people, as well as data that allows for re-identification of victims of gender-based violence are two examples of protection-specific concerns that might be exacerbated by the use of ICT as they might render such information more easily accessible to threat actors.[40] Another protection concern is that of the protection of humanitarian data. For example, the use of social media has become more commonplace in the delivery of services, but this brings with it a number of significant data protection risks such as profiling.[41]

2. Access

Humanitarian access refers to both humanitarian actors' ability to reach populations in need and affected populations' ability to access assistance and services.[42]

The use of ICT can help increase and simplify beneficiaries' access to humanitarian services such as cash assistance, referral services or healthcare. The increased reliance by humanitarians on digital technologies, and the related dependencies on external and internal infrastructure and services, can however bring new challenges.

Access to services can be impeded by the inherent vulnerabilities of the sectors on which organizations and beneficiaries rely (such as healthcare, logistics, banking, and more).[43] The continuity of services in the digital space is not always a given—internet shutdowns and network failures can cause major disruptions to the provision of essential services.[44] In Kenya, such a network failure led to 'occasional delays, disruption or cancellation of the food distribution in the camps, contributing to long queues and crowd control challenges'.[45]

[37] ALNAP (2018). **Incorporating the principle of "Do No Harm": How to take action without causing harm - Reflections on a review of Humanity & Inclusion's practices**.

[38] UNOCHA, **Themes: Protection**.

[39] Sandvik, Jacobsen and McDonald (2017). **Do no harm: A taxonomy of the challenges of humanitarian experimentation**, International Review of the Red Cross (2017), 99 (1), 319-344.

[40] ICRC (2020). **Handbook on Data Protection in Humanitarian Action**.

[41] 'Incidents reported include social engineering attacks such as phishing employed via messaging apps (targeting of Tibetan diaspora via Whatsapp) profiling and targeting of the Tibetan Diaspora through WhatsApp); commercially available spyware used against political dissidents outside of country of origin and for targeting asylum seekers; as well as new vulnerabilities that are being regularly discovered and patched in major messaging services (eg. Whatsapp)' see UNHCR (2021). **Using Social Media in Community Based Protection: A Guide**.

[42] OCHA on Message (April 2017). **Humanitarian Access.**

[43] Fore more on these vulnerabilities and how they are exacerbated by emerging cyber threats, see: UNOCHA GHPF (2022). **Virtual Risk, Tangible Harm: The Humanitarian Implications of Cyber Threats**.

[44] KeepItOn (2019). **The State of Internet Shutdowns around the world. The 2018 #KeepItOn Report**, Access Now for the #KeepItOn coalition.

[45] World Food Programme (WFP)/UNHCR (2014). **Joint Assessment Mission: Kenya Refugee Operation**, Dadaab (23-25 June 2014) and Kakuma (30 June-1 July 2014) Refugee Camps, 2014.

3. Accountability to affected people and communications with communities

Accountability to affected people is an active commitment to use power responsibly by taking account of, giving account to, and being held to account by the people humanitarian organizations seek to assist.[46] Communications with Communities aims to meet the information and communications needs of people affected by crisis.[47]

Ensuring timely and reliable access to and use of information is paramount to AAP and CwC. Increasingly, humanitarians provide this information at least in part through digital channels, either to complement face-to-face services or where physical proximity to communities is not feasible. This dependency on digital services means that cyber operations stand to have grave humanitarian repercussions.

One particular threat related to AAP and CwC is misinformation, disinformation and hate speech, which has become more prevalent with the increased use of ICT.[48] MDH can put affected communities and humanitarian workers at risk by further destabilizing fragile environments, increasing vulnerability and affecting humanitarian organizations' reputation.[49]

Recommendations

Humanitarian organizations should consider the following recommendations to improve cyber resilience.

Invest in cybersecurity as a cross-organizational issue by:

- Integrating cybersecurity into broader organizational frameworks and strategies, including relevant legal, technical and operational safeguards.
- Promoting an active stance from staff at all levels through awareness-raising programmes and displaying an engaged leadership style on cybersecurity matters overall.[50]
- Allocating appropriate long-term and flexible funding for cybersecurity and data responsibility as an integral component of humanitarian programming.
- Advocating for increased investment into the responsible operations of digital technologies to reduce related vulnerabilities.

Enhance institutional preparedness by:

- Identifying and analyzing common cybersecurity challenges including identifying potential threats and threat actors specific to their work, as well as the potential vulnerabilities in their operations and systems.
- Conducting regular risk assessments to identify threats and vulnerabilities, particularly when planning new cyber-enabled activities or exploring new technologies to support activities.
- Implementing several mitigation measures, such as putting in place security standards for hardware and software, and adopting a 'zero trust' approach that favors restrictions such as least-privilege access, microsegmentation and multi-factor authentication.
- Diversifying supply chains to remove strong supplier dependencies, and considering free and open source alternatives (as long as they are approved or appropriately vetted).
- Developing and adapting existing technologies to humanitarian situations, and ensuring contextualized tailoring, testing, efficacy and safety before deployment.

[46] IASC: **Accountability to Affected Populations (AAP) : A brief overview**.

[47] OCHA (2014). **OCHA on Message: Communications with Communities**.

[48] CDAC (2021). **Digital Communication and Accountability: Insights from a year of discussions with CDAC Network**.

[49] International Review of the Red Cross (2020). **Q&A: Humanitarian operations, the spread of harmful information and data protection**. IRRC 102 (913), 27-41.

[50] UN (2021). **Cybersecurity in the United Nations system organizations: Report of the Joint Inspection Unit**.

- Establishing internal and cross-organizational approaches to identifying, resolving, tracking and communicating about data incidents.[51]

Increase digital literacy of staff by:

- Dedicating appropriate resources and funding for training and awareness raising efforts.
- Engaging and training staff and stakeholders regularly to help build cybersecurity into everyday working practices.
- Building digital literacy of humanitarian actors through cross-sector hires and upskilling.
- Increasing data literacy to enable staff to adopt responsible practices and improve their cyber hygiene, including practicing good password management, using anti-virus/anti-malware software and avoiding phishing scams.[52]

Improve coordination and collaboration by:

- Creating an environment that fosters a culture of coordination, collaboration and information sharing among actors.
- Integrating into wider public and private sector cybersecurity communities, ensuring they participate in threat intelligence analysis and information-sharing channels, including disclosure.
- Partnering with relevant stakeholders to improve cybersecurity and humanitarians' access to new areas of expertise and technologies.[53]
- Supporting existing initiatives, systems and projects, for example promoting interoperable data sharing platforms with adequate protections for personal and sensitive data within and across organizations and sectors.
- Communicating about initiatives, threat scanning and potential breaches to highlight the issue of cybersecurity and support the development of a knowledge base, fostering a more coordinated approach to incident management over time.

The **Centre for Humanitarian Data** ('the Centre'), together with key partners, is publishing a set of guidance notes and tip sheets on Data Responsibility in Humanitarian Action over the course of 2022 and 2023. These complement the Centre's series of **guidance notes** and **tip sheets**, as well as the **Inter-Agency Standing Committee Operational Guidance on Data Responsibility in Humanitarian Action** and the **OCHA Data Responsibility Guidelines**, which were published in February 2021 and October 2021 respectively. Through the series, the Centre aims to support continued engagement from different stakeholder groups around high-level commitments and collective action on data responsibility. These guidance notes have been made possible with the support of the Government of Switzerland.

This *Guidance Note on the Humanitarian Implications of Cyber Threats* builds on OCHA's publications on cyber related issues in the humanitarian sector, including *Humanitarianism in the Age of Cyber-warfare: Towards the Principled and Secure Use of Information in Humanitarian Emergencies* and the 2022 Overview Paper on Virtual Risk, Tangible Harm: The Humanitarian Implications of Cyber Threats.[54]

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Foreign Affairs FDFA

[51] Centre for Humanitarian Data (2019). **Guidance Note on Data Incident Management**.

[52] Centre for Humanitarian Data (2022). **Guidance Note on Data Security in Operational Data Management**.

[53] Centre for Humanitarian Data (2020). **Guidance Note on Data Responsibility in Public-Private Partnerships**.

[54] UNOCHA GHPF (2022). Virtual Risk, **Tangible Harm: The Humanitarian Implications of Cyber Threats**.